ICAM

Identity, Credential,
& Access Management

Federal Identity, Credential, and Access Management Trust Framework Solutions

Functional Requirements

For

FICAM SAML 2.0 Web Browser SSO Profile v1.0.2

Version 1.0.0

Table of Contents

1. INTRODUCTION

This document lists the functional requirements for *Federal Identity, Credentialing, and Access Management Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile* v 1.0.2 [FICAM SAMLSSO]. In addition to requirements the document establishes an "expected result" for each requirement. The expected result is used to determine the success of respective tests against each requirement. Requirements and expected results apply to both SAML Relying Party (RP) and Credential Service Provider (CSPs) or Token Manager (TM) and can be used to test software products, libraries, services, and agency implementations to ensure conformance [FICAM SAMLSSO].

The requirements in the [FICAM SAMLSSO] are written specifically for Federal Agency deployments. However requirements can be applied to product testing as well. In some cases the expected result contains special instructions or caveats, in italics, when a product is under test. Optional elements for deployments MUST be supported by product vendors.

Additionally, requirements are organized into "conformance modes", which are subsets of requirements applicable to a given actor in SAML 2.0 transactions. This is intended to make it simpler for agency implementations and product vendors to focus testing on areas of greatest relevance to their situation.

Conformance Mode	Applicable Sections
Relying Party	• Sections 2.1.1, 2.1.2, 2.1.3 • Sections 3.1.1-3.1.4
Credential Service Provider / Token Manager	• Sections 2.1.1, 2.1.2, 2.1.4 • Sections 4.1.1-4.1.4
Metadata Authority	• Section 5.1.1

2. TESTING FOR METADATA

2.1 Metadata Test Scenarios

Conformance test procedures are designed to address each metadata requirement in [FICAM SAMLSSO] and apply to both CSPs/TMs and RPs.

2.1.1 RP and CSP/TM Metadata Consumption Tests

Attempt to install each of the sample metadata product under test.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
M2.0	3.3.3.1	Required	ICAM member implementations MUST support at least one of the following metadata import mechanisms:. • 3.3.3.1.a: Local file (e.g., obtained out of band). • 3.3.3.1.b: Remote resource at fixed location accessible via HTTP 1.1 [RFC 2616] over SSL v3 or TLS 1.1 (and higher) [RFC 2818].
			Expected Result: Test Passes if at least one of the import methods in 3.3.3.1.a or 3.3.3.1.a is successful. Document which method(s) the RP supports for metadata consumption.
M2.1	3.3.3.1.b.i.	Optional	For metadata consumption, In the case of HTTP resolution, ICAM member implementations SHOULD support use of the "`ETag`" header for cache management.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the import of sample metadata was successful and whether or not the RP under test attempted to refresh at the appropriate time.
M2.2	3.3.3.1.b.iii	Optional	ICAM member implementations MAY import metadata from more than one source.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not two or more of the metadata files have successfully imported and maintained
M2.3	3.3.3.2	Required	At consumption time, the metadata consumer MUST perform XML-signature verification at the root element level.
			Expected Result: Test Passes if the RP under test rejects Sample Metadata.
M2.4	3.3.3.3	Required	At consumption time, the metadata consumer MUST support one of the mechanisms for establishment of signature key trust from 3.3.3.3.a or 3.3.3.3.b • 3.3.3.3.a. Direct comparison against preconfigured keys. • 3.3.3.3.b. Does RP support path-based certificate validation against one or more trusted root certificates combined with either certificate revocation list (CRL) or online certificate status protocol (OCSP).
			Expected Result: Test Passes if Sample Metadata are successfully consumed. Document which method of signature key trust are supported.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
M2.5	3.3.3.4	Required	The `validuntil` attribute in an `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` element MUST be honored. ICAM members MUST refresh the metadata before it is expired. If for some reason the metadata cannot be refreshed before it expires, the member MUST make a risk-based determination whether or not to continue transacting with the effected entities.
			Expected Result: Test Passes if the RP under test provides some notification that Sample Metadata has expired or attempts to acquire it automatically
M2.6	3.3.3.5	Optional	Metadata consumers SHOULD be capable of processing one or more consolidated metadata per section 3.3.2.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not two or more of the sample metadata have been successfully imported and maintained

2.1.2 RP and CSP/TM Metadata Exchange

Validate metadata capabilities.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
M2.7	3.3.1.1	Required	ICAM Member metadata MUST include at least one `<md:EntityDescriptor>` element.
			Expected Result: Test Passes if the Metadata from the RP under test has at least one `<md:EntityDescriptor>` element.
M2.8	3.3.1.1.a	Required	`<md:EntityDescriptor>` MUST contain a unique entity-id.
			Expected Result: Test Passes if the entity descriptor contains a unique entity id. *For product testing the uniqueness condition is not tested.*
M2.9	3.3.1.1.b	Optional	`<Organization>` SHOULD be present and include `OrganizationName` or `OrganizationDisplayName`.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the metadata from the RP under test includes <Organization>, `OrganizationName` and/or `OrganizationDisplayName`
M2.10	3.3.1.1.c	Required	`validUntil` and `cacheDuration` Attributes MUST be present and their values set using risk-based methods.
			Expected Result: Test Passes if `validUtil` and `cacheDuration` attributes are present Document the values
M2.11	3.3.1.1.c.i	Recommended	It is RECOMMENDED that `cacheDuration` not exceed 64800 seconds (18 hours).
			Expected Result: Test Passes even if recommendation is not supported,

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			Document whether or not `cacheDuration` is less than or equal to 64800
M2.12	3.3.1.1.d	Required	Prior to metadata distribution, the `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` MUST be digitally signed with an ICAM-approved certificate.
			Expected Result: Test Passes of the metadata produced by the RP under test contains a digital signature. *For product testing, the certificate need not be ICAM approved.*
M2.13	3.3.1.1.e	Required	`<md:KeyDescriptor>` MUST include a `<ds:KeyInfo>` with one `<ds:X509Certificate>` element as a child of `<ds:X509Data>.`
			Expected Result: Test Passes if the metadata from the RP under test contains `<ds:KeyInfo>` within `<ds:X509Data>` which is within `<md:KeyDescriptor>`
M2.14	3.3.1.1.e.i	Required	Other sub elements of `<ds:KeyInfo>` are permitted (e.g., `<ds:KeyValue>`) but they MUST all represent the same key.
			Expected Result: Test Passes if each subelement of `<ds:KeyInfo>` all contain the same certificate

2.1.3 RP Metadata Exchange

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
M2.15	3.3.1.2	Required	RPs MUST include a `<md:SPSSODescriptor>` in their `<md:EntityDescriptor>` element.
			Expected Result: Test Passes if the metadata from the RP under test includes a `<md:SPSSODescriptor>` in their `<md:EntityDescriptor>` element.
M2.16	3.3.1.2.a	Required	`protocolSupportEnumeration` MUST be present and MUST include *urn:oasis:names:tc:SAML:2.0:protocol* .
			Expected Result: Test Passes if `protocolSupportEnumeration` is present and includes *urn:oasis:names:tc:SAML:2.0:protocol*
M2.17	3.3.1.2.b	Required	`WantAssertionsSigned` MUST be set to true.
			Expected Result: Test Passes of `WantAssertionsSigned` is present and set to true
M2.18	3.3.1.2.c	Optional	If the RP uses Assertion encryption, `<md:SPSSODescriptor>` MUST contain at least one `<md:KeyDescriptor>.`
			Expected Result: Test Passes if the metadata from the RP under test uses Assertion encryption and contains at least one `<md:KeyDescriptor>`., or if Assertion encryption is not used. *Products MUST support this feature.*
M2.19	3.3.1.2.d	Optional	`<md:SPSSODescriptor>` MAY contain `<md:SingleLogOutService>`.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not `<md:SPSSODescriptor>` contains `<md:SingleLogOutService>.`
M2.20	3.3.1.2.e	Optional	`<md:SPSSODescriptor>` MAY contain <md:AttributeConsumingService>. *Products MUST support*

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			this feature.
			Expected Result: Document whether or not `<md:SPSSODescriptor>` contains `<md:AttributeConsumingService>`.
M2.21	3.3.1.2.e.i	Optional	RPs wishing to request attributes in an `<samlp:AuthnRequest>` MUST publish one or more `<md:AttributeConsumingService>` in their metadata that includes the set of desired attributes.
			Expected Result: Test Passes of the metadata from the RP under test contains one or more `<md:AttributeConsumingService>` which includes a set of attributes
M.2.22	3.1.0.6	Required	One or more `<md:AssertionConsumerService>` MUST be present in with `Location` attribute set.
			Expected Result: Test Passes if RP metadata contains or more `<md:AssertionConsumerService>` MUST be present in with `Location` attribute set.

2.1.4 CSP/TM Metadata Exchange

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
M2.23	3.3.1.3	Required	IdPs MUST include `<md:IDPSSODescriptor>` in their `<md:EntityDescriptor>` element.
			Expected Result: Test Passes if CSP/TM Metadata contains the `IDPSSODescriptor` element in the `EntityDescriptor` element.
M2.24	3.3.1.3.a	Required	`protocolSupportEnumeration` MUST be present and MUST include *urn:oasis:names:tc:SAML:2.0:protocol*.
			Expected Result: Test Passes if `protocolSupportEnumeration` is present and includes *urn:oasis:names:tc:SAML:2.0:protocol*
M2.25	3.3.1.3.b	Required	`<md:IDPSSODescriptor>` MUST contain at least one `<md:KeyDescriptor>`
			Expected Result: Test Passes if `IDPSSODescriptor` element contains at least one `KeyDescriptor` element.
M2.26	3.3.1.3.c.	Required	One or more `<md:SingleSignOnService>` MUST be present in `<md:IDPSSODescriptor>`. Binding MUST be set to *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect* or *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST*
			Expected Result: Test Passes if at least one `SingleSignOnService` element is present in `IDPSSODescriptor` and for each the binding is set to redirect or post.
M2.27	3.3.1.3.d	Optional	`<md:IDPSSODescriptor>` MAY contain `<md:AttributeAuthorityDescriptor>`.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not `IDPSSODescriptor` contains `AttributeAuthorityDescriptor.`
M2.28	3.3.1.3.d.i	Optional	IdPs SHOULD include <Attribute> within <md:AttributeAuthorityDescriptor> for attributes they are capable of sharing.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the CSP/TM metadata includes one or more Attribute elements within `AttributeAuthorityDescriptor`.
M2.29	3.3.1.3.e.	Required	`<md:EntityDescriptor>` MUST include the CSP/TM's LOA expressed in accordance with OASIS `Expressing Identity Assurance in SAML 2.0`, Section 3 [Assurance]
			Expected Result: Test Passes of the CSP/TM metadata `EntityDescriptor` includes at least LOA4.
M2.30	3.3.1.3.e.i.	Required	The LOAs expressed in metadata MUST contain the highest LOA the CSP/TM is certified to assert.
			Expected Result: Test Passes of the CSP/TM metadata `EntityDescriptor` includes at least LOA2.
M2.31	3.3.1.3.e.ii	Optional	The CSP/TM SHOULD list all the LOA's it is certified to assert in metadata.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not each of the LOA1-2 are included in the CSP/TM metadata.

3. TESTING FOR SAML RELYING PARTIES

Conformance test procedures are designed to address requirements for Relying Parties (RPs) in [FICAM SAMLSSO].

3.1.1 Relying Party Assertion Request Processing

Validate SAML assertion request processing by the RP.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
Rp3.1	3.1.1	Required	The `<samlp:AuthnRequest>` MUST include a `<saml:Issuer>` element matching the EntityID in the metadata of the RP.
			Expected Result: Test Passes if the `AuthnRequest` includes an Issuer element which matches the `EntityID` in the RP metadata
Rp3.2	3.1.1.a	Required	The `EntityID` MUST be a URL that is in the RP's control.
			Expected Result: Test Passes if the `EntityID` is an RP endpoint.
Rp3.3	3.1.2	Recommended	Omitting `<saml:Subject>` and `<saml:Conditions>` from `<samlp:AuthnRequest>` is RECOMMENDED.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not `Subject` or `Conditions` elements are present in the request.
Rp3.4	3.1.3	Recommended	Omitting `<saml:Scoping>` from `<samlp:AuthnRequest>` is RECOMMENDED.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not a `Scoping` element is included in the request.
Rp3.5	3.1.4	Required	`ForceAuthn` MUST be supported.
			Expected Result: Test Passes if the Authn request contains `ForceAuthn`=true
Rp3.6	3.1.5	Required	isPassive MUST be supported.
			Expected Result: Test Passes of the Authn request contains `isPassive`=false
Rp3.7	3.1.7 3.1.7.b	Required	`<samlp:AuthnRequest>` MUST include `<samlp:RequestedAuthnContext>` with one or more `<saml:AuthnContextClassRef>`s .
			Expected Result: Test Passes if the `AuthnRequest` includes `RequestedAuthnContext` with one or more `AuthnContextClassRef.` The value of at least one `<saml:AuthnContextClassRef>` element MUST be one of the following ICAM Assurance URLs: For interacting with a CSP: • http://idmanagement.gov/ns/assurance/loa/1 • http://idmanagement.gov/ns/assurance/loa/2

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			• http://idmanagement.gov/ns/assurance/loa/3 • http://idmanagement.gov/ns/assurance/loa/4 For interacting with a TM: • http://idmanagement.gov/ns/assurance/tal/1 • http://idmanagement.gov/ns/assurance/tal/2 • http://idmanagement.gov/ns/assurance/tal/3 • http://idmanagement.gov/ns/assurance/tal/4 The following URIs are allowed but depreciated: • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel4
Rp3.8	3.1.7.a	Required	The value of the Comparison operator MUST be set to "`exact`" unless RP and CSP/TM have previously negotiated the use of other operators.
			Expected Result: Test Passes if the `Comparison` attribute of the `RequestedAuthnContext` element is set to "exact"
Rp3.9	3.1.8 3.1.8.a	Required	`<samlp:NameIDPolicy>` Format MUST be present.
			Expected Result: Test Passes if `NameIDPolicy` is present and set to one of the following values: `<samlp:NameIDPolicy>` Format MUST be set to one of the following: • *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent* • *urn:oasis:names:tc:SAML:2.0:nameid-format:transient* • *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified*
Rp3.10	3.1.9	Required	The `<samlp:AuthnRequest>` issued by the RP MUST be communicated to the CSP/TM using the HTTP-REDIRECT or HTTP-POST binding.
			Expected Result: Test Passes if the RP uses the redirect or post binding
Rp3.11	3.1.10	Optional	For compatibility reasons, `<samlp:AuthnRequest>` SHOULD be signed.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the `AuthnRequest` is signed.
Rp3.12	3.1.11	Optional	Validate. If present, `<samlp:AuthnRequest>` `ProtocolBinding` MUST be set to *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST*.
			Expected Result: Test Passes if `ProtocolBinding` is present and the binding is HTTP Post; Test

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			Passes if `ProtocolBinding` is not present.
Rp3.13	3.1.12	Optional	`AttributeConsumingServiceIndex` MAY be included in the `<samlp:AuthnRequest>` in order to indirectly indicate a set of attributes the RP desires.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not there is an `AttributeConsumingServiceIndex` in the request
Rp3.14	3.4.1.a	Recommended	The use of TLS 1.2 is RECOMMENDED.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not TLS 1.2 or SSL v.3.
Rp3.15	3.4.1.b	Recommended	It is RECOMMENDED that the TLS implementation conform to [NIST SP 800-52].
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the negotiated cipher suites are allowed in [NIST SP 800-52].

3.1.2 Relying Party Assertion Response Processing

Validate SAML assertion response processing by the RP.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
Rp3.16	3.2.1.a	Required	If received, RPs MUST process an unsolicited `<samlp:Response>` s.
			Expected Result: The RP accepts and unsolicited assertion.
Rp3.17	3.2.1.b	Required	RPs SHOULD accept `<saml:Assertion>`s only from IdPs whose `EntityIDs` are found in metadata.
			Expected Result: The RP *rejects* an assertion from and CSP/TM whose EntityID is unknown.
Rp3.18	3.2.2	Required	The *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST* binding MUST be supported.
			Expected Result: Test Passes if the RP processes responses delivered using HTTP POST binding.
Rp3.19	3.2.3	Required	The <*samlp:Response*> MUST include a <*saml:Issuer*> element whose value matches the *EntityID* for the CSP/TM in metadata
			Expected Result: The RP *rejects* a response from and CSP/TM whose EntityID is unknown.
Rp3.20	3.2.6 3.2.6a	Required	<*saml:AuthnContext*> MUST be present in the assertion with exactly one <*saml:AuthnContextClassRef*> elements. For a CSP: • http://idmanagement.gov/ns/assurance/loa/1 • http://idmanagement.gov/ns/assurance/loa/2

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			• http://idmanagement.gov/ns/assurance/loa/3 • http://idmanagement.gov/ns/assurance/loa/4 For a TM: • http://idmanagement.gov/ns/assurance/tal/1 • http://idmanagement.gov/ns/assurance/tal/2 • http://idmanagement.gov/ns/assurance/tal/3 • http://idmanagement.gov/ns/assurance/tal/4 The following URIs are allowed but depreciated: • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel4
			Expected Result: The RP processes a response from and CSP/TM with AuthnContext value matches the AuthnContext value in the Authentication Request.
Rp3.21	3.2.6.b	Optional	The RP SHOULD compare the LOA in the Response with the LOA in the CSP/TM's metadata, and end the transaction if the LOA in the Assertion is higher than the LOA for the CSP/TM published in metadata.
			Expected Result: Test Passes even if recommendation is not supported,
Rp3.22	3.2.0.8.f.	Optional	RPs SHOULD NOT accept `<saml:Assertion>`s containing attributes that have not been negotiated out of band or via metadata.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the RP under test accepts the assertion and rejects the user login.
Rp3.23	3.4.1	Required	SSL v3 or TLS 1.1 (and higher) MUST be used to protect all protocol endpoints.
			Expected Result: Test Passes if the Third Party CSP/TM receives the `Authn` request, since it only presents SSL-protected endpoints.
Rp3.24	3.4.3	Required	The RP MUST validate that the key used to sign the `<saml:Assertion>` matches the key in the metadata for that `EntityID` in the `<saml:Assertion>`.
			Expected Result: Test Passes if the RP validates the assertion signature.

3.1.3 SLO Start at RP

Configure the RP under test for single logout.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
Rp.3.25	3.5.1	Optional	The RP SHOULD offer the end user a choice between simple logout (logging out only from the RP) and SLO.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the RP under test offers a choice of logout.
Rp3.26	3.5.1.a	Optional	When SLO is initiated at the RP, the `<LogoutRequest>` SHOULD be communicated over SSL v3 or TLS 1.1 (and higher), and use the HTTP Redirect binding.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the RP sends a `<LogoutRequest>` to the Third Party CSP/TM and whether or not it uses the HTTP redirect binding.
Rp3.27	3.5.3.3	Optional	Upon receiving `<LogoutRequest>`, an RP SHOULD terminate the end user's RP session.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the RP under test terminates the end users session
Rp3.28	3.5.4.3.a	Optional	Otherwise, the recipient of `<LogoutResponse>` SHOULD inform the end user that he or she has logged out successfully
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the RP under test informs the end user that they have been logged out

3.1.4 RP SSO with LOA 4 Holder of Key

If product support for HoK is offered, the following tests are required. Otherwise these tests are optional.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
Rp3.30	3.2.1.3	Required	The RP MUST verify that the end user possesses the private key to the certificate that is referenced in the holder-of-key assertion using a LOA 4 protocol as specified in [NIST SP 800-63-1] Section 9, Authentication Process.
			Expected Result: Test Passes if the RP redirects the tester to the CSP/TM to re-authenticate.
Rp3.31	3.2.1.3.i	Required	Validate Furthermore the RP must validate that the certificate issuer is cross-certified with the Federal Bridge Certification Authority.
			Expected Result: Test Passes if the RP validates the user's certificate in the returned assertion.

4. TESTING FOR SAML CSPS/TMS

Conformance test procedures are designed to address requirements for CSP/TM in [FICAM SAMLSSO].

4.1.1 Credential Service Provider / Token Manager Assertion Request Processing

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
IdP4.1	3.1.1	Required	The `<samlp:AuthnRequest>` MUST include a `<saml:Issuer>` element matching the EntityID in the metadata of the RP.
			Expected Result: Test Passes if the CSP/TM rejects an `AuthnRequest` which includes an unknown Issuer element.
IdP4.2	3.1.4	Required	`ForceAuthn` MUST be supported.
			Expected Result: Test Passes if the CSP/TM does not force the user to authenticate and sends an error assertion to the RP.
IdP4.3	3.1.5	Required	`isPassive` MUST be supported.
			Expected Result: Test Passes if the CSP/TM does not force the user to authenticate and sends an error assertion to the RP.
IdP4.4	3.1.6.a	Optional	If `AssertionConsumerServiceURL is` present in `<samlp:AuthnRequest>,` the CSP/TM SHOULD compare the `AssertionConsumerServiceURL` with the requestor's metadata, and MUST end the transaction if there is no match
			Expected Result:Document whether the CSP/TM compares the `AssertionConsumerServiceURL` with the requestor's URL from metadata.
IdP4.5	3.1.7.b	Required	The value of at least one `<saml:AuthnContextClassRef>` element MUST be one of the following ICAM LOA URLs: For a CSP: • http://idmanagement.gov/ns/assurance/loa/1 • http://idmanagement.gov/ns/assurance/loa/2 • http://idmanagement.gov/ns/assurance/loa/3 • http://idmanagement.gov/ns/assurance/loa/4 For a TM: • http://idmanagement.gov/ns/assurance/tal/1 • http://idmanagement.gov/ns/assurance/tal/2 • http://idmanagement.gov/ns/assurance/tal/3 • http://idmanagement.gov/ns/assurance/tal/4

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			The following URIs are allowed but depreciated: • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3 Other ICAM-approved LOA URL value **Expected Result**: Test Passes if a positive assertion is formulated in response to an AuthnRequest containing at least one `AuthnContextClasRef`, and value in response matches value in request.
IdP4.6	3.1.8 3.1.8.a	Required	`<samlp:NameIDPolicy>` Format MUST be present. **Expected Result**: Test Passes if a positive assertion is formulated in response to a request containing AuthnRequest `NameIDPolicy` set to one of the following values: • *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent* • *urn:oasis:names:tc:SAML:2.0:nameid-format:transient* • *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified*
IdP4.7	3.1.9	Required	The `<samlp:AuthnRequest>` issued by the RP MUST be communicated to the CSP/TM using the HTTP-REDIRECT or HTTP-POST binding. **Expected Result**: Test Passes if a positive assertion is formulated in response to an AuthnRequest sent using the redirect *and* post binding
IdP4.8	3.1.10	Required	For compatibility reasons, `<samlp:AuthnRequest>` SHOULD be signed. **Expected Result**: Test Passes if a positive assertion is formulated in response to a signed AuthnRequest.
IdP4.9	3.1.12	Required	`AttributeConsumingServiceIndex` MAY be included in the `<samlp:AuthnRequest>` in order to indirectly indicate a set of attributes the RP desires. **Expected Result**: Test Passes if a positive assertion is formulated in response to an AuthnRequest containing an `AttributeConsumingServiceIndex`.

4.1.2 *Credential Service Provider / Token Manager Assertion Response Processing*

Validate SAML assertion request processing by the RP.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
IdP4.10	3.2.1	Optional	Validate. An CSP/TM MAY send unsolicited `<samlp:Response>`s .

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the CSP/TM under test sends an unsolicited assertion to the Third Party RP, and the tester is logged in at LOA1.
IdP4.11	3.2.2	Required	The *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST* binding MUST be supported.
			Expected Result: Test Passes if the CSP/TM sends the assertion back to the Third Party CSP/TM using POST.
IdP4.12	3.2.3	Required	The <samlp:Response> MUST include a <saml:Issuer> element whose value matches the EntityID for the CSP/TM in metadata.
			Expected Result: Test Passes if the EntityID matches the assertion Issuer element.
IdP4.13	3.2.4.a	Required	If the authentication request is successful, <samlp:Response> MUST contain exactly one <saml:Assertion> or one <saml:EncryptedAssertion>.
			Expected Result: Test Passes if there is only one Assertion or EncryptedAssertion element.
IdP4.14	3.2.4.b	Required	If the authentication request is successful, <samlp:Response> MUST be sent via a protected session (i.e., SSL/TLS) Footnote 12: See Section 3.4 for implementation details
			Expected Result: Test Passes if the Third Party RP receives the assertion since all endpoints are protected by SSL.
IdP4.15	3.2.5	Required	The <saml:Assertion> MUST contain exactly one <saml:AuthnStatement>.
			Expected Result: Test Passes if the assertion contains one and only one AuthnStatement.
IdP4.16	3.2.5.a	Optional	<saml:AuthnStatement> SessionIndex parameter SHOULD be present.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the SessionIndex parameter is present.
IdP4.17	3.2.5.b	Optional	<saml:AuthnStatement> SessionNotOnOrAfter MAY be present.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not SessionNotOnOrAfter is present.
IdP4.18	3.2.6	Required	<saml:AuthnContext> MUST be present with exactly one <saml:AuthnContextClassRef> elements.
			Expected Result: Test Passes if assertion contains AuthnContext with exactly one AuthnContextClassRef.
IdP4.19	3.2.6.a	Required	The value of <saml:AuthnContextClassRef> element MUST be set to one of the following ICAM LOA URLs: For a CSP: • http://idmanagement.gov/ns/assurance/loa/1 • http://idmanagement.gov/ns/assurance/loa/2 • http://idmanagement.gov/ns/assurance/loa/3

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			• http://idmanagement.gov/ns/assurance/loa/4 For a TM: • http://idmanagement.gov/ns/assurance/tal/1 • http://idmanagement.gov/ns/assurance/tal/2 • http://idmanagement.gov/ns/assurance/tal/3 • http://idmanagement.gov/ns/assurance/tal/4 The following URIs are allowed but depreciated: • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2 • http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3 Other ICAM-approved LOA URL value
			Expected Result: Test Passes if the assertion `AuthnContextClassRef` is populated with ICAM LOA URIs.
IdP4.20	3.2.7	Required	The `<saml:Assertion>` MUST contain a `<saml:Subject>.`
			Expected Result: Test Passes if the assertion contains a Subject element.
IdP4.21	3.2.7.a	Required	`<saml:Subject>` MUST contain a `<saml:NameID>`.
			Expected Result: Test Passes if the Subject element contains a `NameID` element.
IdP4.22	3.2.7.b	Required	For Authentication transactions between citizens and government, `<saml:NameID>` Format in the response MUST be either of the following: *urn:oasis:names:tc:SAML:2.0:nameid-format:transient* *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent* *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*
			Expected Result: Test Passes if the `NameId` format is one of the acceptable values.
IdP4.23	3.2.7.b.1	Recommended	The use of pseudonyms (persistent identifiers) is strongly RECOMMENDED
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the assertion contains a pseudonym or real name in the `NameID` element.
IdP4.24	3.2.8	Required	The `<saml:Assertion>` MUST contain zero or one `<saml:AttributeStatement>`s.
			Expected Result: Test Passes even if recommendation is not supported, Document the contents of each of the `AttributeStatement` elements.
IdP4.25	3.2.8.a	Required	Each `<saml:AttributeStatement>` MUST contain one or more `<saml:Attribute>`s, which MAY contain any number of <saml:AttributeValue>s.
			Expected Result: Test Passes if each `AttributeStatement` contains one or more Attribute elements.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
			Document whether or not any of the Attribute elements contain `AttributeValue` elements.
IdP4.26	3.2.8.b	Required	The CSP/TM MUST set the value of the `NameFormat` attribute to *urn:oasis:names:tc:SAML:2.0:attrname-format:uri*.
			Expected Result: Test Passes if the NameFormat attribute is the required value.
IdP4.27	3.2.8.c	Required	`<saml:AttributeStatement>` MUST use `<saml:Attribute>` and MUST NOT use `<saml:EncryptedAttribute>`.
			Expected Result: Test Passes if there are no `EncryptedAttribute` elements in the assertion.
IdP4.28	3.2.8.d	Recommended	The use of URI-formatted Attribute names from well-known registries is RECOMMENDED.
			Expected Result: Test Passes even if recommendation is not supported, Document the attribute names in the assertion.
IdP4.29	3.2.8.e	Required	IdPs MUST NOT send attributes that are not requested by the RP.
			Expected Result: Test Passes if there are no additional attributes aside from those requested by the Third Party RP.
IdP4.30	3.2.9	Required	The `<saml:Assertion>` MUST include a `<saml:Conditions>.`
			Expected Result: Test Passes if the assertion contains a `Condition` element.
IdP4.31	3.2.10. 3.4.2	Required	The <saml:Assertion> MUST be digitally signed.
			Expected Result: Test Passes if the assertion is signed.
IdP4.32	3.4.1	Required	SSL v3 or TLS 1.1 (and higher) MUST be used to protect all protocol endpoints.
			Expected Result: Test Passes if the Third Party RP receives the assertion since all endpoints are protected by SSL.
IdP4.33	3.4.1.a	Recommended	The use of TLS 1.2 is RECOMMENDED.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not TLS is used instead of SSL v3.
IdP4.34	3.4.1.b	Recommended	It is RECOMMENDED that the TLS implementation conform to [NIST SP 800-52].
			Expected Result: Test Passes even if recommendation is not supported, Document the cipher suite negotiated in the SSL session, and document whether or not this is approved in [NIST SP800-52].
IdP4.35	3.4.5	Recommended	The use of SHA1 hashes for signatures is NOT RECOMMENDED.
			Expected Result: Test Passes even if recommendation is not supported, Document the hashing algorithm used in the digital signature on the assertion.
IdP4.36	3.4.5.a	Recommended	The use of SHA256 is RECOMMENDED
			Expected Result: Test Passes even if recommendation is not supported, Document the hashing algorithm used in the digital signature on the assertion.

4.1.3 SLO Start at CSP/TM

If product support for Single Log Out (SLO) is offered, the following tests are required. Otherwise these tests are optional.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
IdP4.38	3.5.2	Optional	If the end user logs out while at an CSP/TM resource, the CSP/TM SHOULD terminate the end user's authentication session
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the tester is logged out of the CSP/TM under test.
IdP4.39	3.5.2.i	Optional	If the end user logs out while at an CSP/TM resource, the CSP/TM SHOULD initiate SLO (i.e., terminate all RP sessions associated with that authentication session).
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the CSP/TM under test sends a logout request to the Third Party RP and is logged out at this RP.
IdP4.40	3.5.2.a	Optional	Before proceeding, the CSP/TM SHOULD inform the end user that he or she will be logged out of all active RP sessions, and the end user SHOULD confirm the request. `<Logout Request>`
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the tester receives notification from the CSP/TM under test that the logout will be for all active RP sessions, and whether or not the tester is asked to confirm.
IdP4.41	3.5.3.1	Optional	`<LogoutRequest>` SHOULD be signed.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the CSP/TM under test sends a signed `<LogoutRequest>`
IdP4.42	3.5.3.2	Optional	Upon receiving `<LogoutRequest>`, an CSP/TM SHOULD send `<LogoutRequest>` to every RP associated with the authentication session - except for the RP that submitted `<LogoutRequest>` to the CSP/TM since that RP already logged out the end user.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the CSP/TM under test sends a logout request to additional RPs.
IdP4.43	3.5.3.4	Optional	The CSP/TM SHOULD log the end user out locally (i.e., terminate the authentication session) and send a `<LogoutResponse>` to the originating RP to indicate SLO completion.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the tester is logged out of the CSP/TM under test.
IdP4.44	3.5.4.1.i	Optional	The `<LogoutResponse>` SHOULD be sent using the HTTP Redirect binding.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the HTTP Redirect binding is used.
IdP4.45	3.5.4.2	Optional	`<LogoutResponse>` SHOULD be signed.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not the `LogoutResponse` is signed.
IdP4.46	3.5.4.1	Required	`<LogoutResponse>` MUST be communicated over SSL v3 or TLS 1.1 (and higher).
			Expected Result: Validate that the `LogoutResponse` reaches the Third Party RP, since there is non-SSL endpoint.

4.1.4 CSP/TM SSO with LOA 4 Holder of Key

If product support for HoK is offered, the following tests are required. Otherwise these tests are optional.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
IdP4.47	3.2.0.7.c.i	Optional	For holder-of-key assertions, the Method attribute of `<saml:SubjectConfirmation>` MUST be *urn:oasis:names:tc:SAML:2.0:cm:holder-of-key*
			Expected Result: Test Passes if method is holder of key.
IdP4.48	3.2.1.1	Optional	The end user MUST authenticate to the CSP/TM using a certificate whose issuer is cross-certified with the Federal Bridge Certification Authority or issued under the Common Policy Framework Certification Authority at a certificate policy that meets the requirements of LOA 4 (See [FBCA CP] or [CPFCA CP]).
			Expected Result: The tester is able to log in to the CSP/TM under test using test user certificate #8.
IdP4.49	3.2.1.2	Optional	Holder-of-key assertions may be used at LOA 4 provided that the following requirements are met: The CSP/TM MUST generate a holder-of-key assertion that references the LOA 4 certificate that the end user used to authenticate to the CSP/TM.
			Expected Result: Test Passes if the assertion contains the LOA4 test certificate #8.
IdP4.50	3.2.1.2.a	Optional	Holder-of-key assertions may be used at LOA 4 provided that the following requirements are met: The value of at least `one <saml:AuthnContextClassRef>` element MUST be: http://idmanagement.gov/ns/assurance/loa/4
			Expected Result: Test Passes if LOA4 is present in the assertion.
IdP4.51	3.2.1.2.b	Optional	Holder-of-key assertions may be used at LOA 4 provided that the following requirements are met: The value of the Method attribute of `<saml:SubjectConfirmation>` MUST be *urn:oasis:names:tc:SAML:2.0:cm:holder-of-key*.
			Expected Result: Test Passes if the method is holder of key.
IdP4.52	3.2.1.2.b.i	Optional	Holder-of-key assertions may be used at LOA 4 provided that the following requirements are met: The `<saml:SubjectConfirmation>` element MUST include a `<ds:KeyInfo>` with one `<ds:X509Certificate>` element as a child of `<ds:X509Data>`.
			Expected Result: Test Passes if X509Certificate element is present as a child of `X509Data`.
IdP4.53	3.2.1.2.b.ii	Optional	Holder-of-key assertions may be used at LOA 4 provided that the following requirements are met: The `<ds:X509Certificate>` element MUST contain the certificate that the end user used to authenticate to the CSP/TM.
			Expected Result: Test Passes if the `X509Certificate` element contains test user certificate #8

5. TESTING FOR ICAM METADATA AUTHORITIES

5.1.1 Consolidated Metadata Validation

Extract the consolidated RP metadata and CSP/TM metadata.

Test ID	Profile ID	Scope	Functional Requirement and Expected Result
MA.1	3.3.2.1	Optional	Validate. ICAM MAY consolidate `<md:EntitiesDescriptor>` metadata files issued by other organizations into one `<md:EntitiesDescriptor>` file for ICAM use.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not there is a single `EntitiesDescriptor` element or multiple.
MA.2	3.3.2.1.a.i	Optional	Validate. The root element MAY contain one or more `<md:EntitiesDescriptor>` elements.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not there are one or more `EntitiesDescriptor` subelements of the root `EntitiesDescriptor` element.
MA.3	3.3.2.1.a.ii	Optional	Validate. The root element MAY also contain one or more `<md:EntityDescriptor>` elements.
			Expected Result: Test Passes even if recommendation is not supported, Document whether or not there are one or more `EntityDescriptor` subelements of the root `EntitiesDescriptor` element.
MA.4	3.3.2.1.i	Optional	Validate. Support for the use of nested `<md:EntitiesDescriptor>` elements in a single file is REQUIRED
			Expected Result: Test Passes if there are nested `EntitiesDescriptor` elements in either the RP or CSP/TM metadata.
MA.5	3.3.2.1.a.	Optional	Validate The root element of consolidated metadata MUST be `<md:EntitiesDescriptor>`.
			Expected Result: Test Passes if the root element for both the RP and CSP/TM metadata is `EntitiesDescriptor`.
MA.6	3.3.2.1.b	Optional	Validate. ICAM MUST digitally sign the root `<md:EntitiesDescriptor>` and all its contents.
			Expected Result: Test Passes if there is a valid signature on the `EntitiesDescriptor` root element.
MA.7	3.3.2.1.c	Optional	Validate. `validUntil` attribute MUST be present.
			Expected Result: Test Passes if `validUntil` is present and has a valid date
MA.8	3.3.2.1.c.i	Optional	Validate. `cacheDuration` attribute MUST be present.
			Expected Result: Test Passes if `cacheDuration` is present and contains a valid duration.

6. Appendix A – Reference Documentation

[AuthnContext] Expressing Identity Assurance in SAML 2.0
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf

[FICAM SAMLSSO] "Federal Identity, Credentialing, and Access Management Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile", Version 1.0.3
http://www.idmanagement.gov/documents/SAML20_Web_SSO_Profile.pdf

[FIPS 140] Federal Information Processing Standards Publication 140-2; Security Cryptographic Modules
http://csrc.nist.gov/publications/nistpubs/

[NIST SP 800-52] Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations (NIST Special Publication 800-52)
http://csrc.nist.gov/publications/nistpubs/

[NIST SP 800-63-1] Electronic Authentication Guideline; National Institute of Science and Technology (NIST Special Publication 800-63-1)
http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[OMB M-04-04] E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) Memorandum M-04-04
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[RFC 2218] HTTP Over TLS
http://www.ietf.org/rfc/rfc2818.txt

[RFC 2616] Hypertext Transfer Protocol.
http://www.ietf.org/rfc/rfc2616.txt

[SAML2 Profiles] "Profiles for the OASIS Security Markup Language (SAML) V2.0", Oasis Standard, 15 March 2005. Document Identifier: saml-profiles-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[Scheme Adoption] ICAM Identity Scheme Adoption Process
http://www.idmanagement.gov/documents/IdentitySchemeAdoptionProcess.pdf

[Services Guide] Third Party ICAM SAML 2.0 SSO Conformance Internet-Accessible Services Guide
[TBD]

[SimpleSAMLphp] SimpleSamlPHP is an open source library that allows SAML IdPs and RPs to run on Apache Web Server.
http://simplesamlphp.org/

APPENDIX B – ACRONYMS

Acronym	Definition
FICAM	Federal Identity, Credential and Access Management
HTTP	Hypertext Transfer Protocol
ICAM	Identity, Credential and Access Management
CSP	Credential Service Provider
TM	Token Manager
LOA	Level Of Assurance
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
RFC	Request for Comment
RP	Relying Party
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer
TBD	To Be Determined
TLS	Transport Layer Security
URL	Uniform Resource Locator
XML	eXtensible Markup Language